REMARKS/ARGUMENTS

The Office Action mailed April 7, 2004 has been carefully considered. Reconsideration in view of the following remarks is respectfully requested.

Regarding Amendments

The abstract has been amended to correct minor errors noted in the Office Action. These corrections are of a clerical nature and do not add "new matter".

Claim Status and Amendment to the Claims

Claims 71, 74, and 77 have been cancelled, without prejudice or disclaimer of the subject matter contained therein.

Claims 1-70, 72-73, and 75-76 are now pending.

No claims stand allowed.

The 35 U.S.C. §112 Rejection

Claims 71, 74, and 77 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter

which the Applicant regards as the invention.[1] With this Amendment, claims 71, 74, and 77 have been cancelled without prejudice or disclaimer, thus rendering the 35 U.S.C §112 moot.

The 35 U.S.C. §102 Rejection

Claims 1-77 stand rejected under 35 U.S.C. §102(a) as being allegedly anticipated by Chan et al.[2], among which claims 1, 9, 27, 45, 46, 53, 58, 59, 64, 69, 72, and 75 are independent claims.[3] This rejection is respectfully traversed.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.[4] The identical invention must be shown in as complete detail as is contained in the claim.[5]

Claim 1 recites:

> A method for remote incremental program verification, said method comprising: receiving content verified by at least one content provider, said at least one content provider including an applet provider, a device manufacturer and a device issuer, said content including at least one program unit, each program unit comprising an Application Programming Interface (API) definition file and an implementation, each API definition file defining items in its associated program unit that are made accessible to one or more other

[1] Office Action dated April 7, 2004, ¶ 5.
[2] USP 6,005,942.
[3] Office Action ¶ 6.
[4] *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ 2d 1051, 1053 (Fed. Cir. 1987).
[5] *Richardson v. Suzuki Motor Co.*, 869 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). See also, M.P.E.P. §2131.

program units, each implementation including executable code corresponding to said API definition file, said executable code including type specific instructions and data;
installing said content on a resource-constrained device;
disabling subsequent installation of content on said resource-constrained device; and
issuing said resource-constrained device to an end user.

The Examiner states:

As per claim 1, (Chan, Fig 3A, col 4 lines 59-67, col 7 lines 22-25, co 10 lines 27-30, col 19 lines 25-30, col 18 lines 30-40, col 3 lines 30-40, col 16 lines 7-15, col 11 lines 1-5).[6]

The Applicant respectfully disagrees. Contrary to the Examiner's statement, Chan et al. does not disclose receiving content verified by at least one content provider, where the content comprises at least one program unit, and where each program unit comprises an Application Programming Interface (API) definition file *and* an implementation. Rather, Chan et al. discloses:

> The applet Install File must contain all information that is required by the card in order to receive the applet, store it in non volatile storage and make it ready to run. This mandatory data includes the following: name or identifier of the applet; identification of hardware and software requirements (version of virtual machine, system class and system framework); link references to libraries and classes in ROM that need to be resolved; link references to libraries/class/functions in non volatile that need to resolved; link references within the applet that need to be resolved; fix ups for data references that need to be resolved; entry points for "process" and "install" methods; and proof of ownership, origin, and completeness and correctness. Optional information includes memory requirements, debug information and any potential terminal related information.
>
> The applet development process begins as soon as a concept of the desired applet is formulated. Once formulated, the concept must go through a number of

[6] Office Action ¶ 6.

> stages before becoming a full fledged working and installable applet. An applet consists of two primary elements; the applet's process method; and the applet's install method. The applet development process (executable) is considered complete after creating and securely delivering the Install File. This development process may vary by organization but in general consists of the following steps: applet requirements gathering and definition; applet specification is developed from requirements; source code is developed from specification; managing applet source code, testing, approving; translate applet source code into card executable code; conversion to card byte code; card byte code verification; code linking and reference resolution; and signature creation.
>
> The results of the translation process is the Install File. *The Install File contains the card byte code that is to be executed by the card.* The purpose of this file may be one or more of the following: input to the ROM image (masking); input to tho initialization procedure (pre issuance load); and distribution for post issuance load (Secure Install). The Install File format and its contents are target system independent. The result of an applet development process is a target system independent signed Install File that contains the complete information need for loading an applet onto a card. *The applet executable is contained within a single Install File.* This Install File can be used for any of the following: the masking process; the initialization process; or the Secure Install process.[7]

Thus, Chan et al. discloses an "Install File" that contains card byte code that is to be executed by the card. Whereas claim 1 requires that the received content comprises at least one program unit, and that each program unit comprises *both* an API definition file *and* an implementation. Claim 1 further specifies that the API definition file defines items in its associated program unit that are made accessible to one or more other program units. This is not shown in Chan et al. in as complete detail as required by claim 1.

[7] Chan et al. col. 19 line 31 to col. 20 line 10. (emphasis added)

Claim 1 also requires disabling subsequent installation of content on said resource-constrained device. This is not shown in Chan et al. in as complete detail as required by claim 1.

Claims 45, 58, and 69

Claims 45, 58, and 69 also include substantially the same distinctive features as claim 1. Claim 1 being allowable, claims 45, 58, and 69 must also be allowable.

Claims 9, 46, 59, and 72

Like claim 1, claims 9, 46, 59, and 72 require that the received content comprises at least one program unit, and that each program unit comprises *both* an API definition file *and* an implementation. Thus, the argument made for claim 1 applies here as well. Claim 1 being allowable, claims 9, 46, 59, and 72 must also be allowable.

Additionally, claims 9, 46, 59, and 72 recite in part allowing post-issuance installation of verified content on a resource-constrained device by a trusted post-issuance installer. This is not shown in Chan et al. in as complete detail as required by claim 1. In fact, Chan et al. does not distinguish between a trusted post-issuance installer and an untrusted post-issuance installer. For this additional reason, the 35 U.S.C. § 102 rejection of claims 9, 46, 59, and 72 is unsupported by the art and must be withdrawn.

Claims 27, 53, 64, and 75

Like claim 1, claims 27, 53, 64, and 75 require that the received content comprises at least one program unit, and that each program unit comprises *both* an API definition file *and* an implementation. Thus, the argument made for claim 1 applies here as well. Claim 1 being allowable, claims 27, 53, 64, and 75 must also be allowable.

Additionally, claims 27, 53, 64, and 75 recite in part allowing post-issuance installation of verified content on a resource-constrained device by an untrusted post-issuance installer. This is not shown in Chan et al. in as complete detail as required by claim 1. In fact, Chan et al. does not distinguish between a trusted post-issuance installer and an untrusted post-issuance installer. For this additional reason, the 35 U.S.C. § 102 rejection of claims 27, 53, 64, and 75 is unsupported by the art and must be withdrawn.

Dependent Claims 2-8, 10-26, 28-44, 47-52, 54-57, 60-63, 65-68, 70, 73, and 76

Claims 2-8 depend from claim 1. Claims 10-26 depend from claim 9. Claims 28-44 depend from claim 27. Claims 47-52 depend from claim 46. Claims 54-57 depend from claim 53. Claims 60-63 depend from claim 59. Claims 65-68 depend from claim 64. Claims 70, 73, and 76 depend from claims 69, 72, and 75, respectively. Claims 1, 9, 27, 46, 53, 59, 64, 69, 72, and 75 being allowable, claims 2-8, 10-26, 28-44, 47-52, 54-57, 60-63, 65-68, 70, 73, and 76 must also be allowable for at least the same reasons.

Claims 2, 14, and 32

Claims 2, 14, and 32 require that the verification be performed by an applet provider. In support of the contention that Chan et al. discloses this limitation, the Examiner cites a portion of Chan et al. that discusses a process performed by the "Card Domain".[8] However, the "Card Domain" in Chan et al. is an application on the smart card that manages the card.[9] It makes no reference to an applet provider. For this additional reason, the 35 U.S.C. § 102 rejection of claims 2, 14, and 32 is unsupported by the art and must be withdrawn.

Claims 3, 15, and 33

Claims 3, 15, and 33 require that the verification be performed by a device manufacturer. In support of the contention that Chan et al. discloses this limitation, the Examiner cites a portion of Chan et al. that discusses a process performed by a card personalization agent and a smart card issuer.[10] It makes no reference to a device manufacturer. Furthermore, the process described by Chan et al. is not verification. Rather, the process described by Chan et al. includes deploying the smart card to customers, deciding whether to install an application on the smart card, initiating a dialogue between the smart card issuer and the smart card, and forwarding a signed copy

[8] Chan et al. col. 24 lines 25-35.
[9] Chan et al. Abstract.
[10] Chan et al. col. 16 lines 6-15.

of an application to the smart card. No verification step performed by the smart card issuer is disclosed. For this additional reason, the 35 U.S.C. § 102 rejection of claims 3, 15, and 33 is unsupported by the art and must be withdrawn.

Claims 4, 16, and 34

Claims 4, 16, and 34 require that the verification be performed by a device issuer. In support of the contention that Chan et al. discloses this limitation, the Examiner cites a portion of Chan et al. that discusses a process performed by a card personalization agent and a smart card issuer.[11] However, the process described by Chan et al. is not verification. Rather, the process described by Chan et al. includes deploying the smart card to customers, deciding whether to install an application on the smart card, initiating a dialogue between the smart card issuer and the smart card, and forwarding a signed copy of an application to the smart card. No verification step performed by the smart card issuer is disclosed. For this additional reason, the 35 U.S.C. § 102 rejection of claims 4, 16, and 34 is unsupported by the art and must be withdrawn.

Claims 5, 17, and 35

Claims 3, 15, and 33 require that the verification be performed by an applet provider and a device manufacturer. In support of the contention that Chan et al. discloses this limitation, the Examiner cites a portion of Chan et al. that discusses a

[11] Chan et al. col. 16 lines 6-15.

process performed by a card personalization agent and a smart card issuer.[12] It makes no reference to a device manufacturer or an applet provider. Furthermore, the process described by Chan et al. is not verification. Rather, the process described by Chan et al. includes deploying the smart card to customers, deciding whether to install an application on the smart card, initiating a dialogue between the smart card issuer and the smart card, and forwarding a signed copy of an application to the smart card. No verification step performed by the smart card issuer is disclosed. For this additional reason, the 35 U.S.C. § 102 rejection of claims 5, 17, and 35 is unsupported by the art and must be withdrawn.

Claims 6, 18, and 36

Claims 6, 18, and 36 require that the verification be performed by an applet provider and a device issuer. The arguments made above with respect to claims 2, 14, and 32, and with respect to claims 4, 16, and 34, apply here.

Claims 7, 19, and 37

Claims 7, 19, and 37 require that the verification be performed by a device manufacturer and a device issuer. The arguments made above with respect to claims 3, 15, and 33, and with respect to claims 4, 16, and 34, apply here.

[12] Chan et al. col. 16 lines 6-15.

Claims 8, 20, and 38

Claims 8, 20, and 38 require that the verification be performed by an applet provider, a device manufacturer, and a device issuer. The arguments made above with respect to claims 2, 14, and 32, with respect to 3, 15, and 33, and with respect to claims 4, 16, and 34, apply here.

Claims 10, 47, and 60

Claims 10, 47, and 60 require that the trusted post-issuance installer verifies a new program unit and installs the verified new program unit on a resource-constrained device. In support of the contention that Chan et al. discloses this limitation, the Examiner cites a portion of Chan et al. that discusses a signature verification process performed by a card domain application executing in a smart card[13]. Thus, the Chan et al. reference discloses verifying a *signature*, not verifying a *program unit* as required by claims 10, 47, and 60. For this additional reason, the 35 U.S.C. § 102 rejection of claims 10, 47, and 60 is unsupported by the art and must be withdrawn.

Claims 11, 25, 29, 43, 48, 55, 61, and 66

Claims 11, 29, 48, 55, 61, and 66 require that the post-issuance verification is performed on a resource-rich device. In support of the contention that Chan et al. discloses this limitation, the Examiner cites a portion of Chan et al. that discusses a

[13] Chan et al. col. 15 lines 26-30, and col. 20 lines 42-50.

signature verification process performed by a card domain application executing in a smart card[14], not a resource-rich device as required by claims 11, 29, 48, 55, 61, and 66. For this additional reason, the 35 U.S.C. § 102 rejection of claims 11, 29, 48, 55, 61, and 66 is unsupported by the art and must be withdrawn.

Claims 12, 26, 30, 44, 49, 56, 62, and 67

Claims 12, 30, 49, 56, 62, and 67 require that the post-issuance verification is performed on a terminal device. In support of the contention that Chan et al. discloses this limitation, the Examiner cites a portion of Chan et al. that discusses APDU (Application Protocol Data Unit) interfaces used to communicate between a card acceptance device ("terminal") and a smart card[15]. The reference makes no mention of performing verification on the terminal device as required by claims 12, 30, 49, 56, 62, and 67. For this additional reason, the 35 U.S.C. § 102 rejection of claims 12, 30, 49, 56, 62, and 67 is unsupported by the art and must be withdrawn.

Claims 13, 31, 50, 57, 63, and 68

Claims 13, 31, 50, 57, 63, and 68 require that verification is performed by the provider of the new program unit. In support of the contention that Chan et al. discloses this limitation, the Examiner cites a portion of Chan et al. that discusses a signature

[14] Chan et al. col. 15 lines 26-30, and col. 20 lines 42-50.
[15] Chan et al. col. 5 lines 25-35.

verification process performed by a card domain application executing in a smart card[16]. Thus, the Chan et al. reference discloses *signature* verification by a *smart card*, not *program unit* verification by the *provider* of the program unit as required by claims 13, 31, 50, 57, 63, and 68. For this additional reason, the 35 U.S.C. § 102 rejection of claims 12, 31, 50, 57, 63, and 68 is unsupported by the art and must be withdrawn.

Claim 21

Claim 21 requires that the verification be performed by an applet provider, a device manufacturer, a device issuer, and a trusted post-issuance installer. The arguments made above with respect to claims 8, 20, and 38, and with respect to claims 10, 47, and 60 apply here.

Claim 22

Claim 22 requires that the verification be performed by a device manufacturer, a device issuer, and a trusted post-issuance installer. The arguments made above with respect to claim 7, and with respect to claims 10, 47, and 60 apply here.

Claim 23

Claim 23 requires that the verification be performed by a device manufacturer and

[16] Chan et al. col. 22 lines 1-7.

a trusted post-issuance installer. The arguments made above with respect to claim 3, and with respect to claims 10, 47, and 60 apply here.

Claim 24

Claim 24 requires that the verification be performed by a device issuer and a trusted post-issuance installer. The arguments made above with respect to claim 4, and with respect to claims 10, 46, and 60 apply here.

Claims 28, 54, and 65

Claims 28, 54, and 65 require that the untrusted post-issuance installer verifies a new program unit and installs the verified new program unit on a resource-constrained device. In support of the contention that Chan et al. discloses this limitation, the Examiner cites a portion of Chan et al. that discusses a signature verification process performed by a card domain application executing in a smart card[17]. Thus, the Chan et al. reference discloses verifying a *signature*, not verifying a *program unit* as required by claims 28, 54, and 65. For this additional reason, the 35 U.S.C. § 102 rejection of claims 28, 54, and 65 is unsupported by the art and must be withdrawn.

Claim 39

Claim 39 requires that the verification be performed by an applet provider, a

[17] Chan et al. col. 15 lines 26-30, and col. 20 lines 42-50.

device manufacturer, a device issuer, and an untrusted post-issuance installer. The arguments made above with respect to claims 8, 20, and 38, and with respect to claims 28, 54, and 65 apply here.

Claim 40

Claim 40 requires that the verification be performed by a device manufacturer, a device issuer, and an untrusted post-issuance installer. The arguments made above with respect to claim 7, and with respect to claims 28, 54, and 65 apply here.

Claim 41

Claim 41 requires that the verification be performed by a device manufacturer and an untrusted post-issuance installer. The arguments made above with respect to claim 3, and with respect to claims 28, 54, and 65 apply here.

Claim 42

Claim 42 requires that the verification be performed by a device issuer and an untrusted post-issuance installer. The arguments made above with respect to claim 4, and with respect to claims 28, 54, and 65 apply here.

The Examiner is reminded that the mere absence from a reference of an explicit requirement of a claim cannot be reasonably construed as an affirmative statement that

the requirement is in the reference.[18] For this reason, the 35 U.S.C. § 102 of claims 1-77 is unsupported by the art and should be withdrawn.

Accordingly, it is respectfully requested that the rejection of claims under 35 U.S.C. § 102 be withdrawn. In view of the foregoing, it is respectfully asserted that the claims are now in condition for allowance.

If, in the opinion of the Examiner, an interview would expedite the prosecution of this application, the Examiner is invited to call the undersigned attorney at the number indicated below.

The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 50-1698.

Respectfully submitted,
THELEN REID & PRIEST, LLP

Dated: July 7, 2004

John P. Schaub
Reg. No. 42,125

Thelen Reid & Priest LLP
P.O. Box 640640
San Jose, CA 95164-0640
Tel. (408) 292-5800
Fax. (408) 287-8040

[18] *In re Evanega*, 829 F.2d 1110, 4 USPQ2d 1249 (Fed. Cir. 1987).